

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-295154

(43)Date of publication of application : 21.10.1994

(51)Int.Cl. G09C 1/00

(21)Application number : 05-082978 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 09.04.1993 (72)Inventor : MIYAJI MITSUKO
TATEBAYASHI MAKOTO

(54) SYSTEM FOR SIGNATURE USING ELLIPTIC CURVE, CERTIFICATION, AND SECRET COMMUNICATION

(57)Abstract:

PURPOSE: To obtain the system which speeds up processing without increasing definition fields while maintaining safety, constitutes the elliptic curve and a base point that facilitate combination with speeded-up processing by an existent additive chain, and has the basis of the safety for a discrete logarithmic problem on the elliptic curve by regarding (p) as a specific prime number and constituting the elliptic curve on a finite field GF(p).

CONSTITUTION: For a positive integer (t) and a small integer α , (p) is set to the prime number which becomes $2t \pm \alpha$, and a group consisting of elements on GF (p) of the elliptic curve E which has the finite field GF (p) as a definition field is denoted as E (GF (p)). When the elliptic curve E which is thus constituted and the base point P are used, the position of the base point P is divided by a large prime number and an MOV reduction method can be evaded, so the safe system is provided. Further, basic arithmetic operation is multiplication on GF (p), so this multiplication is realized faster than multiplication on a general finite field because of the form of $p=2t \pm \alpha$. Further, the multiplication can be speeded up by being combined with the method of the addition chain with ease.

(1) 正整数dの決定

(2) 素数pの生成

(3) 楕円曲線E及びベースポイントPの決定

LEGAL STATUS

[Date of request for examination] 12.11.1998

[Date of sending the examiner's decision of rejection] 25.03.2002

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

THIS PAGE BLANK (USPTO)

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2002-07072

[Date of requesting appeal against examiner's decision of rejection] 24.04.2002

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

THIS PAGE BLANK (USPTO)

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平6-295154

(43)公開日 平成6年(1994)10月21日

(51)Int.Cl.⁵

G 0 9 C 1/00

識別記号

庁内整理番号

F I

技術表示箇所

8837-5L

審査請求 未請求 請求項の数 4 O L (全 5 頁)

(21)出願番号 特願平5-82978

(22)出願日 平成5年(1993)4月9日

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 宮地 充子

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74)代理人 弁理士 小銀治 明 (外2名)

(54)【発明の名称】 楕円曲線を用いた署名、認証及び秘密通信方式

(57)【要約】

【目的】 安全性を保ちながら処理の高速化が定義体の増加なしに実現でき、また既存の加法鎖による高速化との組み合わせも容易できる楕円曲線及びベースポイントを構成し、この楕円曲線上の離散対数問題に安全性の根拠をもつ署名、認証及び秘密通信方式を提供する。

【構成】 正整数 t 及び小さい正整数 α に対して、 p を $2^t \pm \alpha$ となる素数とし、有限体 $GF(p)$ を定義体にもつ楕円曲線 E の $GF(p)$ 上の元で構成される群を $E(GF(p))$ とし、前記 $E(GF(p))$ 上定義された離散対数問題を安全性の根拠にもつ。

(1) 正整数 d の決定



(2) 素数 p の生成



(3) 楕円曲線 E 及びベースポイント P の決定

【特許請求の範囲】

【請求項1】正整数 t 及び小さい正整数 α に対して、 p を $2t \pm \alpha$ となる素数とし、有限体 $GF(p)$ を定義体にもつ楕円曲線 E の $GF(p)$ 上の元で構成される群を $E(GF(p))$ とし、前記 $E(GF(p))$ 上定義された離散対数問題を安全性の根拠にもつことを特徴とする楕円曲線を用いた署名、認証及び秘密通信方式。

【請求項2】 p を正整数 t 及び小さい正整数 α に対して、 $2t \pm \alpha$ と表される素数とし、有限体 $GF(p)$ を定義体にもつ楕円曲線 E の $GF(p)$ 上の元で構成される群を $E(GF(p))$ とすると、 $E(GF(p))$ の元の個数が p になるように前記楕円曲線 E をとることを特徴とする請求項1記載の楕円曲線を用いた署名、認証及び秘密通信方式。

【請求項3】正整数 d を、虚二次体 $Q((-d)^{1/2})$ の類数が小さくなるようにとり、素数 p を、 $4 \times p - 1$ の素因数が $d \times$ 平方数となりかつ、正整数 t 及び小さい正整数 α に対して $2t \pm \alpha$ と表せる素数とし、 d により定まる類多項式 $H_d(x) = 0$ の p を法とした解を j 不変数にもつ有限体 $GF(p)$ を定義体にもつ楕円曲線 E をとることを特徴とする請求項2記載の楕円曲線を用いた署名、認証及び秘密通信方式。

【請求項4】正整数 t に対して、正整数 α は略々 $(2t)/3$ ビットの大きさとし、素数 p を $2t \pm \alpha$ と表せる素数とすることを特徴とする請求項3記載の楕円曲線を用いた署名、認証及び秘密通信方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は情報セキュリティ技術としての暗号技術に関するものであり、特に、楕円曲線を用いて実現された暗号技術に関するものである。

【0002】

【従来の技術】秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行なう方式である。また署名及び認証方式とは、通信相手に通信内容の正当性を示したり、本人であることを証明する通信方式である。この署名、認証及び秘密通信方式には公開鍵暗号とよばれる通信方式がある。公開鍵暗号は通信相手が多数の時、通信相手ごとに異なる暗号鍵を容易に管理するための方式であり、不特定多数の通信相手と通信を行なうのに不可欠な基盤技術である。簡単に説明すると、これは暗号化鍵と復号化鍵が異なり、復号化鍵は秘密にするが、暗号化鍵を公開する方式である。この公開鍵暗号の安全性の根拠に用いられるものに楕円曲線上の離散対数問題がある。これはニールコブリッツ著「アコースインナンバセオリイアンドクリプトグラフィ」(Neal Koblitz, "A Course in Number Theory and Cryptography", Springer-Verlag, 1987)に詳しく述べられている。楕円曲線上の離散対数問題を以下に述べる。

【0003】楕円曲線の離散対数問題

q を素数べきとし、 $GF(q)$ を有限体とし、楕円曲線 E の $GF(q)$ 上の元で生成される群を $E(GF(q))$ とし、 $E(GF(q))$ の位数が大きな素数で割れる元 P をベースポイントとする。このとき、 $E(GF(q))$ の与えられた元 Q に対して、

$$Q = xP$$

となる整数 x が存在するならば x を求めよ。

【0004】上記の楕円曲線上の離散対数問題は、1991年に考案された楕円曲線上の離散対数問題を有限体上の離散対数問題に帰着させて解く解法をのぞくとサブイクスポーネンシャルな解法が存在しない。この解法は、A. Menezes, S. Vanstone and T. Okamoto, "Reducing Elliptic Curve Logarithm to Logarithms in a Finite Field", STOC 91に詳しく述べられている。MOV帰着法とは、 q を素数べきとし、有限体 $GF(q)$ 上定義された楕円曲線を E とし、 E の $GF(q)$ 上の元で構成される群を $E(GF(q))$ とする。このとき $E(GF(q)) \ni P$ をベースとする楕円曲線上の離散対数問題は、 P の位数と q が互いに素なときには、有限体 $GF(q)$ のある拡大体 $GF(q^r)$ 上の離散対数問題に帰着して解くことができる。特に E がスーパーシンギュラと呼ばれる楕円曲線の場合には有限体 $GF(q)$ の高々6次拡大体 $GF(q^6)$ 上の離散対数問題に帰着して解くことができる。

【0005】そこで、上記解法のMOV帰着法を避けるように楕円曲線を構成する研究が行われるようになった。この方法は色々あるが、例えば、T. Beth, F. Schaefer, "Non Supersingular Elliptic Curves for Public Key Cryptosystems", Eurocrypt 91, 1991、または宮地充子著"On ordinary elliptic curve cryptosystems", abstract of Asiacypt'91、等に詳しくかかれている。これらの方法を用いて構成すると、現時点ではサブイクスポーネンシャルアルゴリズムを与える解法がないため有限体上の離散対数問題と同程度の安全性ならばはるかに小さな定義体で構成することができる。

【0006】ところが楕円曲線の場合、一演算に12、3回の乗算を要求するので、定義体の大きさが小さくなくてもあまり実行速度が速くならない。そこでMOV帰着法を避けることができさらに実行速度を速くするための研究が行われるようになった。

【0007】次に楕円曲線を用いた暗号の実行速度を速くする従来の技術の一つについて述べる。これはコブリッツ著"CM-curves with good cryptographic properties", Crypto'91, 1991に詳しくかかれている。

【0008】従来例

図2は従来例における署名、認証及び秘密通信方式の実行速度を高速にする楕円曲線の構成を示すものである。

【0009】以下同図を参照しながら従来例の手順を説明する。

(1) 楕円曲線の候補の決定

次の二つのGF(2)を定義体にもつアノラマス楕円曲線を考える。

$$【0010】E_1: y^2 + xy = x^3 + x^2 + 1$$

$$E_2: y^2 + xy = x^3 + 1$$

楕円曲線EのGF(2^m)上の元で構成される群E(GF(2^m))とは次のような群である。

$$【0011】E_1(GF(2^m)) = \{x, y \in GF(2^m) \mid y^2 + xy = x^3 + x^2 + 1\} \cup \{\infty\}$$

$$E_2(GF(2^m)) = \{x, y \in GF(2^m) \mid y^2 + xy = x^3 + 1\} \cup \{\infty\}$$

ここで ∞ は無遠点を表す。

(2) 適当な拡大次数mの決定

公開鍵暗号の安全性の根拠となる上述の楕円曲線の離散対数問題はベースポイントである元Pの位数が大きな素因数を持たなければ簡単に解けることが知られている。

【0012】位数が大きな素因数を持つ元Pが存在するための必要十分条件はE(GF(q))の元の個数が大きな素因数を持つことである。

【0013】そこで、(1)に述べた楕円曲線E_iについてその元の個数#E_i(GF(2^m))が大きな素因数を持つようにmを求める。(i=1, 2)

(3) 実際の楕円曲線の構成例

楕円曲線E_iのGF(2^m)上の元で構成される群E_i(GF(2^m))の元の個数を求めその素因数分解を行なった結果m=101のとき、#E₁(GF(2ⁿ))=2×素数p₁

m=131のとき、#E₂(GF(2^m))=4×素数p₂

となることがわかった。また、MOV掃着法により埋め込まれる有限体が十分大きくなることも確かめられる。

【0014】よってE₂(GF(2¹³¹))上の位数が素数p₂となる元をベースポイントPとする楕円曲線上の離散対数問題もしくはE₁(GF(2¹⁰¹))上の位数が素数p₁となる元をベースポイントPとする楕円曲線上の離散対数問題を安全性の根拠にした公開鍵暗号を構成すればよいことが結論づけられる。

【0015】このように構成した楕円曲線は、2^kP (P=(x, y); k=1, 2, 3, 4)の計算が次のように求められる。

$$【0016】2P = P + P$$

$$4P = -(x^2{}^3, y^2{}^3) - (x^2{}^2, y^2{}^2)$$

$$8P = -(x^2{}^3, y^2{}^3) + (x^2{}^5, y^2{}^5)$$

$$16P = (x^2{}^4, y^2{}^4) - (x^2{}^6, y^2{}^6)$$

一方GF(2)の拡大体上の演算は、基底として正規基底を用いると2乗の計算が巡回シフトで実現されるのでハードウェアで実現するときには、実行速度は無視できる。よって、2^kP (k=1, 2, 3, 4)の計算が2回の楕円曲線の足し算で実行できることになり、高速化が望める。また特にE₂では定義体GF(2¹³¹)上の正規基底は最適な正規基底となり、一回の乗算に必要な論理積及び排他的論理和の回数が最小になるので、基

本演算(有限体の乗算)の高速化が望める。

【0017】しかし上記従来例においては、楕円曲線の一回の加法が高速になるというわけではない。このため、より高速にするには、演算を高速にする条件(最適な正規基底をもつ有限体GF(2^m))と安全で2ⁱ倍点(i=1, 2, 3, 4)が簡単になる楕円曲線の条件(アノラマス楕円曲線であつ元の個数が大きな素数で割れる)の両者の条件を満たす楕円曲線を見つける必要がある。しかし両者の条件は包含関係にあるわけではないので、両者を満たす楕円曲線は少なくなる。実際上記の例の場合、E₂(GF(2¹³¹))のほうが、最適な正規基底を用いることができるが、最適な正規基底が存在しないE₁(GF(2¹⁰¹))のほうが小さい定義体で実現できることになる。

【0018】また一般に楕円曲線のkPの計算を高速にする方法の一つに加法鎖の研究がある。これは、有限体のg^kの計算の加法鎖の研究と平行してなされる。これは、予備計算テーブルの持ち方及び計算の順序の工夫を行う研究である。これについては、M. J. Coster, "Some algorithms on addition chains and their complexity", Center for Mathematics and Computer Science Report CS-R9024に詳しい。この方法を用いたkPの計算と、上述の2ⁱ倍点(i=1, 2, 3, 4)が簡単になる方法を用いたkPの計算では、加法鎖を用いたほうが高速に実現され、両方法の組み合わせによる高速化は困難である。

【0019】

【発明が解決しようとする課題】楕円曲線上の離散対数問題を安全性の根拠にした公開鍵暗号は、高速な処理が求められる。従来例1のように特定のcに対しcPが高速になるという方法の場合、一般のkに対しkPを高速にする際、加法鎖の方法と組み合わせて高速にするのが困難である。またcPが高速になる条件と基本演算が高速になる条件の両方を満たす楕円曲線を構成すると定義体が大きくなるという問題が起こる。

【0020】本発明は、これらの従来例における問題点を鑑みて行なわれたもので、安全性を保ちながら処理の高速化が定義体の増加なしに実現でき、また既存の加法鎖による高速化との組み合わせも容易できる楕円曲線及びベースポイントを構成し、この楕円曲線上の離散対数問題に安全性の根拠をもつ署名、認証及び秘密通信方式を提供することを目的とする。

【0021】

【課題を解決するための手段】請求項1に係る署名、認証及び秘密通信方式においては、正整数t及び小さい正整数αに対して、pを2^t±αとなる素数とし、楕円曲線Eを有限体GF(p)上構成する。

【0022】請求項2に係る署名、認証及び秘密通信方式においては、pを正整数t及び小さい正整数αに対して、2^t±αと表される素数とし、有限体GF(p)を定

義体にもつ楕円曲線 E の $GF(p)$ 上の元で構成される群を $E(GF(p))$ とするとき、 $E(GF(p))$ の元の個数が p になるように前記楕円曲線 E を構成する。

【0023】請求項3に係る署名、認証及び秘密通信方式においては、正整数 d を、虚二次体 $Q((-d)^{1/2})$ の類数が小さくなるようにとり、素数 p を、 $4 \times p - 1$ の素因数が $d \times$ 平方数となりかつ、正整数 t 及び小さい正整数 α に対して $2^t \pm \alpha$ と表せる素数とし、楕円曲線 E を、有限体 $GF(p)$ 上で d により定まる類多項式 $H_d(x) = 0$ の p を法とした解を j 不変数にもつように構成する。

【0024】請求項4に係る署名、認証及び秘密通信方式においては、請求項3記載の方式において、上記正整数 α は、正整数 t に対して、略々 $(2t)/3$ ビットの大きさとし、上記素数 p は $2^t \pm \alpha$ と表せる素数とする。

【0025】

【作用】請求項1に係る発明によれば、正整数 t 及び小さい正整数 α に対して、 p を $2^t \pm \alpha$ となる素数とし、有限体 $GF(p)$ を定義体にもつ楕円曲線 E の $GF(p)$ 上の元で構成される群を $E(GF(p))$ とし、前記 $E(GF(p))$ 上定義された離散対数問題を安全性の根拠にもつことを特徴とした楕円曲線を用いて暗号方式が構成される。

【0026】請求項2に係る発明によれば、 p を正整数 t 及び小さい正整数 α に対して、 $2^t \pm \alpha$ と表せる素数とし、有限体 $GF(p)$ を定義体にもつ楕円曲線 E の $GF(p)$ 上の元で構成される群を $E(GF(p))$ とするとき、 $E(GF(p))$ の元の個数が p になるように前記楕円曲線 E をとることを特徴とした楕円曲線を用いて署名、認証及び秘密通信方式がなされる。

【0027】請求項3に係る発明によれば、正整数 d を、虚二次体 $Q((-d)^{1/2})$ の類数が小さくなるようにとり、素数 p を、 $4 \times p - 1$ の素因数が $d \times$ 平方数となりかつ、正整数 t 及び小さい正整数 α に対して $2^t \pm \alpha$ と表せる素数とし、 d により定まる類多項式 $H_d(x) = 0$ の p を法とした解を j 不変数にもつ有限体 $GF(p)$ を定義体にもつ楕円曲線 E の $GF(p)$ 上の元で構成される群を $E(GF(p))$ とし、前記 $E(GF(p))$ 上定義された離散対数問題を安全性の根拠にもつことを特徴とした楕円曲線を用いて暗号方式が構成される。

【0028】請求項4に係る発明によれば、上記正整数 α は、正整数 t に対して、 $(2t)/3$ ビットぐらいの大きさとし、上記素数 p は $2^t \pm \alpha$ と表せる素数であり、その上で安全で高速な署名、認証及び秘密通信方式の構成がなされる。

【0029】

【実施例】図1は本発明の実施例における楕円曲線上の署名、認証及び秘密通信方式の構成を示すものである。以下同図を参照しながら実施例の手順を説明する。

【0030】(1)正整数 d の決定

正整数 d を、虚二次体 $Q((-d)^{1/2})$ の類数が小さくなるようにとる。ここでは $d=11$ とする。なお虚二次体 $Q((-d)^{1/2})$ 及び類数については、シルバーマン著“ザ アリスメチック オブ エリプティック カーブズ” (J. H. Silverman, “The arithmetic of elliptic curves”, Springer-Verlag, 1986) に詳しく述べられている。

【0031】(2)素数 p の生成

素数 p を、 $4p=11 \times$ 平方数となり、かつ正整数 t 及び $(2t)/3$ ビットぐらいの大きさの α に対し $2^t - \alpha$ と表されるようにとる。

【0032】ここでは

$$p = 2^t - \alpha$$

$$t = 128$$

$$\alpha = 89\ 25388\ 84800\ 47273\ 94087$$

ととる。

【0033】(3)楕円曲線 E 及びベースポイント P の決定

有限体 $GF(p)$ を定義体にもち、元の個数が丁度 p 個になる楕円曲線 E は次で与えられる。

$$E: y^2 = x^3 + 12a^3x + 16a^4$$

$$a = 1887\ 65172\ 00252\ 43003\ 83780\ 59753\ 00282\ 08521$$

このとき、 $E(GF(p))$ の元 $P = (0, 4a^2)$ が存在する。

【0035】上記のようにして構成された楕円曲線 E 及びベースポイント P を従来例2の楕円曲線上の署名、認証及び秘密通信方式に用いると、ベースポイント P の位数が大きな素数で割れ、かつMOV掃着法を避けることができるので安全な方式が実現される。さらに方式の実現に要求される基本演算は $GF(p)$ 上の乗法になるので、 $p = 2^t \pm \alpha$ という形から一般の有限体上の乗法に比較して高速に実現できる。また従来例のように特定の c に対し cP の計算が速くなるというものではないので、一般の k に対して kP の計算を高速にする手法である加算鎖の方法と容易に組み合わせることにより高速化が可能になる。またデータ量についても、定義体のデータとして p を覚える代わりに t と α を覚えることができるので、データ量を約 $2/3$ ビットに削減できる。

【0036】なお、上述の実施例は正整数 d を 11 として行ったが、これは勿論他の虚二次体 $Q((-d)^{1/2})$ の類数が小さくなるような正整数なら何でもよい。また、 d に対して条件を満たす素数 p は上述の実施例だけに限定されるのではなく(2)に示した p に関する条件を満たす素数なら何でもよい。

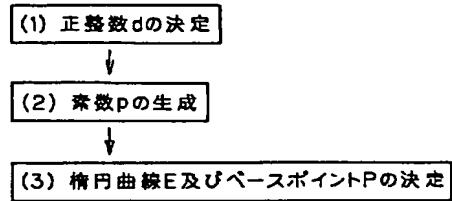
【0037】

【発明の効果】本発明によれば、データ量の削減及び処理の高速化が可能な楕円曲線を構成することができ、高い安全性でより高速な署名、認証及び秘密通信方式の実現が可能になる。

【図面の簡単な説明】

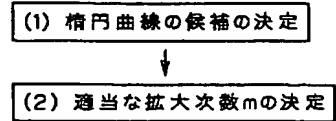
【図 1】 本発明の実施例における楕円曲線の構成図

【図 1】



【図 2】 従来例の楕円曲線の構成図

【図 2】



THIS PAGE BLANK (USPTO)